GB

2008年制定

中国国家标准汇编

389

GB 22186～22237

（2008 年制定）

中国标准出版社　编

中国标准出版社

北　京

图书在版编目（CIP）数据

中国国家标准汇编：2008 年制定．389：GB 22186～22237/中国标准出版社编．—北京：中国标准出版社，2009

ISBN 978-7-5066-5312-1

Ⅰ．中… Ⅱ．中… Ⅲ．国家标准-汇编-中国-2008 Ⅳ．T-652.1

中国版本图书馆 CIP 数据核字（2009）第 082094 号

中国标准出版社出版发行
北京复兴门外三里河北街 16 号
邮政编码：100045

网址 www.spc.net.cn
电话：68523946 68517548
中国标准出版社秦皇岛印刷厂印刷
各地新华书店经销

*

开本 880×1230 1/16 印张 38.75 字数 1 108 千字
2009 年 7 月第一版 2009 年 7 月第一次印刷

*

定价 200.00 元

ISBN 978-7-5066-5312-1
9 787506 653121 >

出 版 说 明

1.《中国国家标准汇编》是一部大型综合性国家标准全集。自1983年起，按国家标准顺序号以精装本、平装本两种装帧形式陆续分册汇编出版。它在一定程度上反映了我国建国以来标准化事业发展的基本情况和主要成就，是各级标准化管理机构，工矿企事业单位，农林牧副渔系统，科研、设计、教学等部门必不可少的工具书。

2.《中国国家标准汇编》收入我国每年正式发布的全部国家标准，分为“制定”卷和“修订”卷两种编辑版本。

“制定”卷收入上一年度我国发布的、新制定的国家标准，顺延前年度标准编号分成若干分册，封面和书脊上注明“20××年制定”字样及分册号，分册号一直连续。各分册中的标准是按照标准编号顺序连续排列的，如有标准顺序号缺号的，除特殊情况注明外，暂为空号。

“修订”卷收入上一年度我国发布的、被修订的国家标准，视篇幅分设若干分册，但与“制定”卷分册号无关联，仅在封面和书脊上注明“20××年修订-1，-2，-3，……”字样。“修订”卷各分册中的标准，仍按标准编号顺序排列（但不连续）；如有遗漏的，均在当年最后一分册中补齐。需提请读者注意的是，个别非顺延前年度标准编号的新制定的国家标准没有收入在“制定”卷中，而是收入在“修订”卷中。

读者配套购买《中国国家标准汇编》“制定”卷和“修订”卷则可收齐上一年度我国制定和修订的全部国家标准。

3. 由于读者需求的变化，自1996年起，《中国国家标准汇编》仅出版精装本。

4. 2008年我国制修订国家标准共5946项。本分册为“2008年制定”卷第389分册，收入国家标准GB 22186～22237的最新版本。

中国标准出版社

2009年5月

目　录

ICS 35.40
L 80

中华人民共和国国家标准

GB/T 22186—2008

信息安全技术 具有中央处理器的集成电路(IC)卡芯片安全技术要求(评估保证级4增强级)

Information security techniques—Security technical requirements for IC card chip with CPU(EAL4+)

2008-07-16 发布　　2008-12-01 实施

中华人民共和国国家质量监督检验检疫总局
中国国家标准化管理委员会　发布

前　言

本标准的附录A是规范性附录。

本标准由全国信息安全标准化技术委员会提出并归口。

本标准主要起草单位：中国信息安全产品测评认证中心。

本标准主要起草人：李守鹏、付敏、杨永生、郭颖、潘莹、高金萍、李蒙、祁斌、闫石、胡兵、李刚、陈冈、许珊琳、郑晓光。

引　言

IC卡芯片应用范围的扩大和应用环境复杂性的增加，要求IC卡芯片具有更强的保护数据能力。

本标准在GB/T 18336—2001中规定的EAL4级安全保证要求组件基础上，增加了模块化组件(ADV_INT)，并且将脆弱性分析要求由可以抵御低等攻击潜力的攻击者发起的攻击(组件AVA_VLA.2)提升到可以抵御中等攻击潜力的攻击者发起的攻击(组件AVA_VLA.3)。

本标准仅给出了IC卡芯片应满足的安全技术要求，对IC卡芯片的具体技术实现方式、方法等不作规定。

信息安全技术
具有中央处理器的集成电路(IC)卡芯片
安全技术要求(评估保证级4增强级)

1 范围

本标准规定了对具有中央处理器的集成电路(IC)卡芯片达到EAL4增强级所要求的安全功能要求及安全保证要求。

本标准适用于IC卡芯片的研制、开发、测试、评估和产品的采购。

2 规范性引用文件

下列文件中的条款通过本标准的引用而成为本标准的条款。凡是注日期的引用文件,其随后所有的修改单(不包括勘误的内容)或修订版均不适用于本标准,然而,鼓励根据本标准达成协议的各方研究是否可使用这些文件的最新版本。凡是不注日期的引用文件,其最新版本适用于本标准。

GB/T 18336.1—2001 信息技术 安全技术 信息技术安全性评估准则 第1部分:简介和一般模型(idt ISO/IEC 15408-1:1999)

GB/T 18336.2—2001 信息技术 安全技术 信息技术安全性评估准则 第2部分:安全功能要求(idt ISO/IEC 15408-2:1999)

GB/T 18336.3—2001 信息技术 安全技术 信息技术安全性评估准则 第3部分:安全保证要求(idt ISO/IEC 15408-3:1999)

3 术语、定义和缩略语

GB/T 18336—2001确立的以及下列术语、定义和缩略语适用于本标准。

3.1 术语和定义

3.1.1

智能卡 smart card

具有中央处理器(CPU)的集成电路卡,即IC卡,是将一个具有中央处理器的集成电路芯片镶嵌于塑料基片中,并封装成卡的形式。从数据传输方式上可分为接触式IC卡和非接触式IC卡。

3.1.2

IC专用软件 IC dedicated software

由IC卡芯片设计者开发并且在集成电路生产者交付之后依然以物理形式存在于智能卡集成电路中的专用软件。这些专用软件通常在生产过程中用于测试,也可以用来提供额外的服务以便于硬件的使用或提供附加的服务。

3.1.3

初始化数据 initialization data

在IC卡芯片制造阶段写入的与制造有关的数据,如IC卡芯片的标识号。

3.1.4

个人化数据 personalization data

在个人化阶段写入的数据。

3.1.5

预个人化数据　pre-personalization data

在预个人化阶段前写入的数据。

3.1.6

嵌入式软件　smartcard embedded software

掩膜在CPU卡内并可运行的软件，其主要功能是控制CPU卡和外界的信息交换，管理智能卡的存储器并完成各种命令的处理。

3.2　缩略语

CAD	卡接收设备(Card Acceptor Device)
CPU	中央处理器(Central Processing Unit)
EAL	评估保证级(Evaluation Assurance Level)
EEPROM	电可擦除可编程只读存储器(Electrically-Erasable Programmable Read-only Memory)
IT	信息技术(Information Technology)
I/O	输入/输出(Input/Output)
IC	集成电路(Integrate Circuit)
PP	保护轮廓(Protection Profile)
RAM	随机存取存储器(Random-access memory)
ROM	只读存储器(Read-only memory)

4　IC卡芯片描述

4.1　概述

带中央处理器的IC卡芯片为实现智能卡功能提供了一个硬件平台。IC卡芯片不但包括由处理单元、安全组件、I/O接口(接触和/或非接触)、易失性和/或非易失性存储器(属于硬件部分)等组成的集成电路，还包括由集成电路设计者/生产者加入的专用软件。这些专用软件通常在生产过程中用于测试，也可以用来提供额外的服务以便于硬件的使用或提供附加的服务(如以库的形式)，但智能卡中的嵌入式软件不属于IC卡芯片组成部分。典型的智能卡产品结构如图1所示：

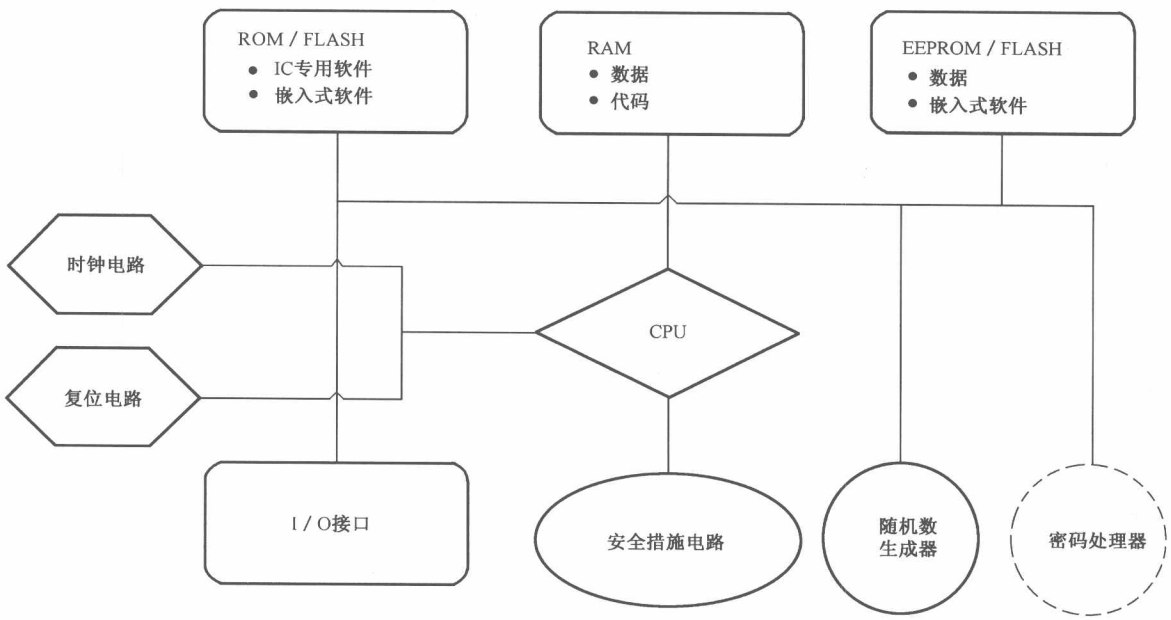

图1　典型的智能卡产品(密码处理器为可选组件)

4.2 特征

4.2.1 IC卡芯片的生命周期

IC卡芯片的生命周期包含在智能卡产品的生命周期之中。智能卡产品的生命周期可分为以下几个阶段，各个阶段内容如表1所示：

表1 智能卡产品的生命周期阶段说明

阶　段	活　动	角　色
阶段1	IC卡芯片开发	IC卡芯片开发者 ● 设计IC卡芯片。 ● 开发IC专用软件。 ● 为嵌入式软件开发者提供IC卡芯片相关信息，软件和开发工具。 ● 通过可信交付和检验接受由开发者提供的智能卡嵌入式软件。 ● 根据IC卡芯片设计，IC专用软件和/或智能卡嵌入式软件的信息，IC卡芯片设计者构造智能卡IC数据库，以便进行IC卡芯片制造。
阶段2	IC卡嵌入式软件开发	IC卡嵌入式软件开发者 ● 智能卡嵌入式软件开发。 ● IC卡预个人化需求说明。
阶段3	IC卡芯片制造与测试	IC卡芯片制造者 ● 通过IC卡芯片制造，IC卡芯片测试，IC卡芯片预个人化三个主要步骤，生产IC卡芯片。 IC掩膜制造者 ● 基于智能卡IC数据库，生产用于IC卡芯片制造的掩膜版。
阶段4	IC卡芯片封装与测试	IC卡芯片封装者 ● IC卡芯片模块封装和测试。
阶段5	制卡	智能卡产品生产者 ● 智能卡产品的成卡和测试。
阶段6	智能卡个人化	个人化管理员 ● 智能卡个人化和最终测试。在个人化阶段嵌入式软件和应用软件下载到智能卡中。
阶段7	智能卡使用阶段	智能卡发行者 ● 将成品智能卡交付给最终用户，以及用户的使用和废弃。

4.2.2 开发环境的特征

开发环境必须设置访问控制策略和严格执行访问控制措施，保证开发过程的可追溯性。

4.2.3 使用环境的特征

IC卡芯片在发行以后，使用环境难以控制，攻击者可能会采用各种手段对IC卡芯片进行攻击，以便获取敏感数据。因此，IC卡芯片必须保证系统内的信息在使用环境下的机密性和完整性。

5 安全环境

5.1 资产

需要保护的资产：

——IC 卡芯片存储和处理的用户数据(例如嵌入式软件所使用的数据)；

——IC 卡芯片存储和处理的安全功能数据(例如安全属性、认证数据、访问控制列表、密钥等)；

——智能卡嵌入式软件；

——IC 专用软件；

——IC 卡芯片的逻辑设计信息，物理设计信息；

——特定的 IC 卡芯片开发辅助工具(例如 ROM 掩膜数据生成工具)；

——与测试和特征有关的数据；

——支持嵌入式软件开发的信息(例如开发资料和开发平台)；

——掩膜版；

——初始化数据和预个人化数据；

——其他与特定功能有关的重要资产(例如 IC 卡芯片产生的随机数)。

在 IC 卡芯片研发、系统生成、数据加载和交付使用过程中必须保证上述资产的机密性、完整性和可用性。

5.2 假设

5.2.1 角色管理(A. Role_Man)

假设角色以一种安全的方式被管理。

IC 卡芯片通常通过对口令的鉴别来确认这些角色，但对角色的管理功能不一定由 IC 卡芯片提供。

5.2.2 CAD 的通信安全(A. CAD_Sec-Com)

假设 IC 卡芯片与 CAD 之间的连接是安全的。

CAD 能够与 IC 卡芯片间建立安全通信的通道。其典型的实现方式是通过共享密钥、公/私钥对，或者利用存储的其他密钥来产生会话密钥。假设当这些安全连接建立以后，IC 卡芯片就可以认为在可信通信中 CAD 是足够安全的。由于 CAD 的安全功能失败而引入的攻击超出了本标准的范围。

5.2.3 IC 卡芯片之外的数据存储(A. Data_Store)

假设存储在 IC 卡芯片之外的 IC 卡芯片数据以一种安全的方式管理。

关于 IC 卡芯片结构、个人化数据、所有者身份等敏感信息将被发行者或其他 IC 卡芯片之外的数据库存储。这些信息一旦泄漏，将危及 IC 卡芯片的安全。因此这些数据得到充分的维护是很重要的。

5.2.4 密钥维护(A. Key_Supp)

假设存储在 IC 卡芯片之外的加密密钥按照一种安全的方式进行维护。

由于使用 IC 卡芯片都可能引入不同的密钥，这些密钥包括共享密钥、公/私钥对等。这些密钥将由执行 IC 卡芯片功能的系统中能够控制操作的实体所提供。假设这些密钥的生成、分发、维护、销毁都是足够安全的。

5.3 威胁

5.3.1 对 IC 卡芯片的威胁

5.3.1.1 物理威胁

5.3.1.1.1 对集成电路的物理探测(T. P_Probe)

攻击者可能对 IC 卡芯片实施物理探测，以获取 IC 卡芯片的设计信息和操作内容。

物理探测可能是利用IC卡芯片失效性分析和采用半导体逆向工程技术来从IC卡芯片中获取数据。这种探测可能包括对电气功能的探测，由于这种探测需要直接接触IC卡芯片内部，所以仍把它归为物理探测。攻击者的目的是获取诸如硬件安全机制、访问控制机制、鉴别系统、数据保护系统、存储器分区，以及密码算法程序等设计细节。弄清软件设计中诸如初始化数据、个人化数据、口令或密钥等也是他们的目标。IC卡芯片可能会在未上电或已上电状态下受到探测攻击并且在遭受这样的攻击后可能会处于无法操作状态。

5.3.1.1.2 **对集成电路的物理更改(T.P_Alter)**

攻击者可能对IC卡芯片实施物理更改，以获取IC卡芯片的设计信息和操作内容，或者改变安全功能及安全功能数据，从而非法使用IC卡芯片。

对IC卡芯片的更改可能是利用IC卡芯片失效性分析或采用半导体逆向工程技术来实现。攻击者的目的是获取诸如硬件安全机制、访问控制机制、鉴别系统、数据保护系统、存储器分区，以及密码算法程序等设计细节。弄清软件设计中诸如初始化数据、个人化数据、口令或密钥等也是他们的目标。更进一步的目标可能是修改或操纵调试阶段的锁定操作、初次使用标记、卡使用锁定、锁定功能配置、卡锁定标志、卡终止标志等，以便非法使用IC卡芯片。

5.3.1.2 **逻辑威胁**

5.3.1.2.1 **缺陷插入(T.Flt_Ins)**

攻击者可能通过反复地插入选定的数据，并观察相应的输出结果，从而获得IC卡芯片安全功能或用户相关的信息。

这种威胁的特点是有目的选择和控制输入数据，而不是随机选择或控制。通过插入选定的数据并观察输出结果的变化，是对密码设备的一种常见攻击手段，这种手段也可用于对IC卡芯片的攻击。其目的是通过观察IC卡芯片如何对选定的输入做出响应来获取与安全功能或用户相关的信息。这种威胁的特点是有意选择和控制输入数据，而不是随机选择数据或控制输入输出操作中的物理特性。

5.3.1.2.2 **错误输入(T.Inv_Inp)**

攻击者可能通过引入无效的输入数据来危及IC卡芯片的安全功能数据的安全。

错误输入操作形式包括错误的格式、索要的信息超过记录范围、试图找到并执行无正式书面文件的命令。这样的输入可能在正常使用过程中的任意时间发生，包括访问授权前。其结果是该攻击可能会危及安全功能、在操作中产生可利用的错误或者泄漏所保护的数据。

5.3.1.2.3 **未授权程序装载(T.Ua_Load)**

攻击者可能利用未授权的程序探测或修改IC卡芯片安全功能代码及数据。

每个授权角色都有特定的权限仅用于下载指定的程序。未授权程序可能包括在正常操作期间不希望执行的合法程序，也可能包括用于有意刺探或修改IC卡芯片安全功能的未授权装载程序。

5.3.1.3 **与访问控制相关的威胁**

5.3.1.3.1 **非法访问(T.Access)**

使用者或攻击者可能在未经信息或资源的拥有者或责任者许可的条件下对信息或资源进行访问。

授权角色都有特定的权限来访问IC卡芯片的信息，如果访问超出规定权限，会导致安全相关信息的暴露。

5.3.1.3.2 **对初始使用权的欺骗(T.First_Use)**

攻击者可能通过未授权使用新的或未发行的IC卡芯片而非法获得IC卡芯片信息。

5.3.1.4 **与不可预测的相互作用相关的威胁**

5.3.1.4.1 **使用被禁止的生命周期功能(T.Lc_Ftn)**

攻击者可能会利用相关命令，尤其是测试和调试命令来获取IC卡芯片安全功能数据或敏感的用户

数据，这些命令在智能卡生命周期的以往某些阶段是必要的，但在现阶段是被禁止的。

这些命令在操作执行的特殊阶段是不必要的或被禁止的。例如在操作阶段使用测试命令或调试命令来显示内存或执行其他功能。

5.3.1.5 **有关密码功能的威胁**

5.3.1.5.1 **密码攻击(T. Crypt_Atk)**

攻击者可能实施密码攻击或穷举攻击危及 IC 卡芯片的安全功能。

这种攻击可能用到一些加密函数、编码/解码函数或随机数发生器。攻击者的目标是发现密码算法中的脆弱性或通过穷举来发现密钥和输入数据。攻击者的目的在于暴露 IC 卡芯片的安全功能数据从而危及用户敏感数据的安全。

5.3.1.6 **监控信息的威胁**

5.3.1.6.1 **信息泄漏(T. I_Leak)**

IC 卡芯片必须提供控制和限制 IC 卡芯片信息泄漏的方法，以免有用的信息暴露在电源、地面、时钟、复位或者 I/O 线路中。攻击者可对正常使用期间 IC 卡芯片泄漏的信息加以利用。

IC 卡芯片必须被设计和编程为，例如通过分析电源消耗不能泄漏处理运算或危及安全的信息。该类泄漏包括功耗、I/O 特性、时钟频率的变化或所需处理时间的变化等。这可理解为一个隐蔽的传输途径，但与操作参数的测量密切相关。这些泄漏信息可通过直接(接触)测量或测量辐射信号得到，并且可能与正在执行的操作有关。能量分析就是一个信息泄漏的例子。

5.3.1.6.2 **综合分析，相关性分析(T. Link)**

攻击者可能观察到一个实体使用的多种资源和服务，联系这些使用，便可推导出这个实体希望保护的安全功能数据。

攻击者综合利用观察到的 IC 卡芯片在一段时间内多次使用的结果，或对不同操作所获取的知识进行综合，就能够得到相关信息，利用这些信息攻击者或者可以直接获取安全信息，或者可以总结出一种攻击手段，进而获取 IC 卡芯片要保护的安全信息。

5.3.1.7 **各种其他威胁**

5.3.1.7.1 **环境压力(T. Env_Strs)**

攻击者可通过将 IC 卡芯片暴露在有压力的环境下来达到向安全功能数据引入错误的目的。

将集成电路暴露在超出其使用范围的情况下，将导致其故障或安全临界元素的失败，从而达到允许操纵程序或数据的目的。这种情况可能是正常参数的极值(高或低)如温度、电压、时钟频率，也可能是不正常的环境如外部能量场。该攻击的目的在于产生一个直接的错误导致安全信息的泄漏，或者是模拟中止进程来产生一个结束使用期限的失败。

5.3.1.7.2 **接续攻击(T. Lnk_Att)**

攻击者在 IC 卡芯片不稳定或其安全功能的某些方面下降时实施后续攻击，从而获取安全功能数据或敏感的用户数据。

5.3.1.7.3 **克隆(T. Clon)**

攻击者可能克隆部分或全部 IC 卡芯片的功能以开发进一步的攻击手段。

攻击者可能通过对 IC 卡芯片本身的详细观察来获取克隆部分或全部 IC 卡芯片所必需的信息。攻击者通过开发 IC 卡芯片的物理模型来实验其不同的功能和处理过程，从而实现进一步的攻击以达到成功暴露安全功能数据和敏感用户数据的目的。

5.3.1.7.4 **IC 卡芯片的更改和重新使用(T. Carrier_Tamper)**

攻击者在原始载体上修改 IC 卡芯片并伪装成原始的 IC 卡芯片从而非法使用用户数据。

移动、修改或者重新将 IC 卡芯片插入到载体中伪装成原始的 IC 卡芯片，其目的在于访问被保护的资产。

5.3.1.7.5 **管理者权力滥用(T. Priv)**

管理者或其他特权用户可能通过执行暴露 IC 卡芯片安全功能或受保护数据的操作而威胁其安全特性。

一个特权用户或管理者可以实施基于上述所有威胁的攻击。

5.4 **组织安全策略**

5.4.1 **数据访问(P. Data_Acc)**

除已定义好的操作集外,对特定数据和客体的访问权限的定义依据:

a) 客体的拥有者;

b) 尝试访问客体的主体标识;

c) 客体的拥有者授予的显式或隐式的访问权限。

IC 卡芯片可能涉及到多个不同的授权者,例如 IC 卡芯片开发者、IC 卡芯片制造者、IC 卡芯片封装者。他们均能以特定的规则或角色访问 IC 卡芯片中的数据。

5.4.2 **标识(P. Ident)**

IC 卡芯片必须被唯一标识。

IC 卡芯片通常包括硬件和专用软件两种元素。专用软件可能是通过硬掩膜存储在 ROM 中或存储在非易失存储器中。硬件具有是否使能的可选特性。一个正确的标识必须是最终 IC 卡芯片产品的精确实例化。需要对每个 IC 卡芯片进行唯一标识。

5.4.3 **密码标准(P. Crypt_Std)**

密码实体、数据鉴别及批准的功能都必须符合国家标准及行业或组织的信息技术安全标准或规范。

5.4.4 **安全通信(P. Sec_Com)**

IC 卡芯片与卡接收设备间的通信应使用安全的协议和程序。

IC 卡芯片可能要进行从简单的状态检查到安全的数据传输等多种通信。至少,IC 卡芯片必须具备为可信的源建立可信信道来加载应用,或执行其他潜在的特权指令。而要一直确保完整性。

6 安全目的

6.1 IC 卡芯片安全目的

6.1.1 **逻辑保护(O. Log_Prot)**

IC 卡芯片应具有抗逻辑操纵或修改的结构,以抵抗逻辑攻击。

IC 卡芯片的设计和编程应达到下述要求:能够抵抗通过对逻辑操作的攻击来威胁安全特性的企图。当 IC 卡芯片受到逻辑探测和命令修改的攻击时,应能保证其内部安全信息不被泄漏。

6.1.2 **防信息泄漏(O. I_Leak)**

IC 卡芯片必须提供控制和限制信息泄漏的方法,使得有用信息不会通过电源、时钟、复位、I/O 线而泄漏。

IC 卡芯片的设计和编程必须达到下述要求:攻击者无法通过分析诸如功耗等因素的变化来获取操作过程的信息或其他安全信息。

6.1.3 **初始化(O. Init)**

IC 卡芯片必须假定在上电、复位或其他重启操作之后必须进入指定初始状态。

无论以何种方式复位,IC 卡芯片都应进入定义好的受控初始状态。此目的应能防止攻击者操纵 IC 卡芯片使其处于未定义的状态。

6.1.4 **防缺陷插入(O. Flt_Ins)**

IC 卡芯片必须能抵御插入缺陷数据重复探测的攻击。